CLAIMS:

1.   A method of granting access to content on a storage medium (101),
comprising obtaining cryptographic data (Y) from a property (102) of the storage medium
(101), reading helper data (W) from the storage medium (101), and granting the access based
on an application of a delta-contracting function to the cryptographic data (Y) and the helper
5   data (W).

2.   The method of claim 1, comprising deriving a decryption key (K) for
decrypting the content at least from the application of the delta-contracting function.

10   3.   The method of claim 2, comprising deriving the decryption key (K) further
from data supplied by a playback or recording apparatus (400).

4.   The method of claim 1, in which the access is granted if the output of the
delta-contracting function corresponds to a control value (V) recorded on the storage medium
15   (101).

5.   The method of claim 4, comprising applying a cryptographic function to the
output of the delta-contracting function and comparing the output of the cryptographic
function to the control value (V).

20

6.   The method of claim 5, in which the cryptographic function is a one-way hash
function.

7.   The method of claim 1, in which the delta-contracting function involves a
25   combination of a matrix multiplication on the cryptographic data (Y), a linear addition of at
least a portion of the helper data (W), a quantization in which the quantization areas are
defined by a portion of the helper data (W), and error correction decoding.

15

8.   A device (110) arranged for granting access to content on a storage medium (101), comprising first reading means (112) for obtaining cryptographic data (Y) from a property (102) of the storage medium (101), second reading means (112) for reading helper data (W) from the storage medium (101), and access control means for granting the access

5   based on an application of a delta-contracting function to the cryptographic data (Y) and the helper data (W).

9.   A playback and/or recording apparatus (400) comprising a device (101) as claimed in claim 8 and arranged to effect the playback and/or recording if access is granted

10   by the device (110).

10.   A computer program product arranged to cause a processor to execute the method of claim 1.